IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

CELLULAR COMMUNICATIONS EQUIPMENT LLC,	§ § §	
Plaintiff,	§	**Case No. 2:20-CV-0078-JRG**
	§	
v.	§	**JURY TRIAL DEMANDED**
	§	
HMD GLOBAL OY,	§ §	
Defendant.	§	

DECLARATION OF ANTHONY DEROSA

TABLE OF CONTENTS

I. Engagement

1. My name is Anthony DeRosa. I understand that Cellular Communications Equipment LLC ("CCE") has sued HMD Global Oy ("HMD") for patent infringement. I have been retained by CCE as a technical consultant in this matter. I am being compensated at my regular hourly rate of $395 per hour for my time. My compensation is in no way tied to the outcome of this matter or to the substance of my opinions.

2. In forming my opinions for this Declaration, I have reviewed U.S. Patent No. 7,218,923 (the "'923 patent"), including its file history. I have also reviewed any documents discussed herein.

3. In reaching my opinions, I have relied on my experience and education in the field. I have also considered the viewpoint of a person having ordinary skill in the art at the time of the earliest claimed priority date for each respective patent.

II. Background

4. I am a computer engineer specializing in the secure design of embedded computing devices and their networks. I am currently the CEO and a principal engineer at Syscall 7. My duties at Syscall 7 include creating and auditing software for wired and wireless telecommunications devices and Android-based mobile devices. I am also the founder of Online Disassembler, a collaborative reverse engineering platform in the cloud.

5. I received my Master of Science in Electrical and Computer Engineering from Johns Hopkins University after receiving my Bachelor of Science in Engineering with a concentration in Computer Engineering from Messiah College.

6. I have worked in the field of computer software, firmware, and embedded systems for nearly eighteen years, gaining experience that spans from the hardware level up through the entire software stack. I served as a computer engineer in the Department of Navy, as a software

developer for multiple technologies. After my time as a civilian in the federal government, I continued supporting the Department of Defense as a federal contractor working for several companies. During this time, I designed, developed, and analyzed a wide range of software and embedded systems, as well as supervising teams of engineers doing the same.

7. In addition to the information provided in this section, additional relevant information related to my education and professional experience is provided in my curriculum vitae, attached to my declaration as Attachment A.

III. Legal Principles

8. I understand that claim construction begins with a focus on the words of the claims themselves, as they would have been understood by a person of ordinary skill in the art at the time of invention. I further understand that, absent some reason to the contrary, claim terms are typically given their ordinary and accustomed meaning as would have been understood by a person having ordinary skill in the art, and my opinions below are rendered from this perspective. I further understand that claim construction focuses mostly on the intrinsic evidence of a patent, which includes the claims, the specification, and the prosecution history.

9. I understand that the Court may also consider extrinsic evidence in the event that the intrinsic evidence does not establish the meaning of a claim. I further understand that examples of this extrinsic evidence are inventor testimony, expert testimony, dictionaries, and learned treatises. I further understand that extrinsic evidence is generally used to provide background on the technology, explain the invention, ensure the Court's understanding of technical aspects is consistent with a person of ordinary skill, or to establish the meaning of a particular claim term in a particular field.

10. I understand that multiple factors should be used to decide the skill level of a person of ordinary skill for a patent, including: the types of problems encountered in the art, the solutions

to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the education level of active workers in the field.

11. I understand that one possible instance in which the Court may depart from the plain and ordinary meaning of a claim term occurs if the patentee has clearly set forth the definition of a disputed term in the specification.

12. I understand that a claim is not indefinite unless the claim, in view of the specification and prosecution history, fails to inform those skilled in the art about the scope of the invention with reasonable certainty. Thus, I understand that a claim term does not require absolute precision, but that the certainty is reasonable, having regard to a claim's subject matter. I understand that whether a claim is indefinite is determined by the perspective of one of ordinary skill in the art as of the time the application for the patent was filed. I further understand that claims are presumed valid, and invalidity due to indefiniteness must be proven by clear and convincing evidence.

13. These legal principles have provided me with the framework for my analysis, and, where applicable, I have relied upon and followed these principles in my analysis. In keeping with the appropriate uses of expert testimony, I have been asked to provide assistance in ensuring that the Court's understanding of technical aspects of the patent-in-suit is consistent with that of a person of ordinary skill in the art, and in establishing that particular terms in the patent-in-suit have particular meanings.

IV. Person Having Ordinary Skill in the Art

14. The field of technology for the '923 patent is related to wireless communications systems and more particularly, messaging systems. In my opinion, a person of ordinary skill in the art of the subject matter of the '923 patent would have been a person having the equivalent of an undergraduate degree in computer science (or a related field) and approximately one year of work

experience in the field of wireless communications systems. Additional education in the field could substitute for industry experience, and vice versa. Under this standard, I am one of at least ordinary skill in the art.

V. Priority Date for the ’923 Patent

15. I understand that the priority date for the ’923 patent is in the early 2000s timeframe, specifically, December 18, 2003. I have used this date in determining the level of skill and knowledge of the relevant person of ordinary skill, which I discussed above.

VI. Disputed Claim Term for U.S. Patent No. 7,218,923 – “a message of the messages” (Claim 1)

CCE’s Construction	HMD’s Construction
one or more, but less than all, of the messages	indefinite

16. Based on my review of the ’923 patent’s claims, specifications, and prosecution history, it is my view that a person of ordinary skill would have readily understood the scope of this term with reasonable certainty. This term would have been understood by a person of ordinary skill to mean one or more of the messages.

17. The term “a message of the messages” uses ordinary language. A person of ordinary skill after considering the intrinsic record would immediately recognize the meaning of this term. Indeed, claim 1 itself provides the context for this claim term:

> A method for controlling application programs in a communication terminal, the method comprising:
>
> ***sending messages from an application program*** towards a communication network, the application program residing in a communication terminal;
>
> ***diverting a message of the messages*** to a controlling entity residing in the communication terminal; and
>
> based on the message, controlling in the controlling entity whether the application program behaves in a predetermined manner in the communication terminal, the

> controlling being performed before the message is transmitted from the communication terminal to the communication network.

’923 Patent at 9:1-22 (emphasis added). As demonstrated by the emphasis in the above, the claim requires sending “messages” (i.e., more than one message) from an application program. Next, “a message” is diverted. I understand that, in patent parlance, an indefinite article “a” carries a meaning of “one or more” in claims that contain the transitional phrase “comprising,” such as claim 1 here. Thus, “one or more” messages of “the messages” introduced in the sending step is diverted. In other words, the claim, as understood by a person of ordinary skill, requires sending multiple messages from an application program and diverting one or more of those messages.

18. This plain reading of the claim is supported throughout the specification, as shown below (all emphasis added):

a. “***At least some of the messages generated by an application*** residing in the terminal and destined for a communication network ***are diverted*** . . . .” ’923 patent at Abstract.

b. “At least some of the outbound messages generated by an application in a terminal are diverted . . . .” ’923 patent at 1:60-63.

c. “***sending messages from an application towards a communication network***, where the application resides in the communication terminal, and ***diverting at least one message destined for the communication network***” ’923 patent at 2:14-18.

d. “The terminal includes one or more ***applications configured to send messages towards a communication network*** and ***diverting means for diverting selected messages*** sent from an application and destined for the communication network to a controlling entity residing in the terminal . . . .” ’923 patent at 2:26-27.

e. “at least one ***application configured to send messages towards the communication network*** and diverting means for ***diverting at least some of the messages sent from an application*** and destined for the communication” ’923 patent at 2:39-41.

Consistent with the description provided by claim 1, the specification describes sending messages from an application and diverting at least one (or at least some or selected) of those sent messages. As such, a person of ordinary skill, after reviewing the intrinsic record would have no doubt that this term means one or more of the messages, wherein "the messages" references the "messages" introduced in the sending step of claim 1.

19. I understand that the Court previously adopted CCE's proposed construction of this term, including the negative limitation of "but less than all." I understand that the reasoning for including the negative limitation in the Court's adopted construction is that a magistrate judge of the Court found that, in a prior IPR proceeding, CCE disclaimed a scope of the claim that would include diverting all of the messages. I have not performed an analysis of whether, in my opinion, CCE did in fact disclaim this claim scope. But, in connection with my opinion, I defer to the Court's prior finding. Accordingly, it is my opinion that "a message of the messages" is properly construed as "one or more, but less than all, of the messages."

20. I understand that, although HMD contends this term is indefinite, HMD has not disclosed any basis for contending the term is indefinite. As such, I reserve the right to respond to any basis that HMD may later provide.

VII. Conclusion

21. I declare under penalty of perjury under the laws of the United States of America that the foregoing statements are true and correct.

Executed on November 25, 2020 in Woodbine, Maryland

Anthony V. DeRosa

Anthony DeRosa

Attachment A

Anthony V. DeRosa

16332 Carrs Mill Rd Woodbine, MD 21797 (410) 671-5389 anthony.derosa@syscall7.com

SUMMARY

Anthony DeRosa is an information security expert specializing in the vulnerability research of networking and embedded computing devices. He has 17 years of experience in reverse engineering using static reverse engineering tools such as IDA Pro, and he is experienced with the runtime debugging environments of GDB, WinDbg, and JTAG-based debuggers like Lauterbach, Green Hills, American Arium, and BDI. Through fuzzing and a combination of static and dynamic reverse engineering, he has uncovered serious vulnerabilities and recommended techniques for securing these systems against the weaknesses uncovered.

Mr. DeRosa is also a full stack software developer, specializing in system-level software development in C and assembly language (x86, MIPS, PowerPC, ARM, NIOS II, and MicroBlaze). With engineering experience that spans from the hardware level up through the entire software stack, he has designed and developed VHDL, debugged hardware with scopes and logic analyzers, developed firmware in C and assembly for multiple embedded platforms, developed OS-level device drivers, developed custom networking protocols, developed GUIs in high-level languages, and developed cloud-based applications using the full stack of web technologies (Django, Bootstrap, AngularJS, Vue.js, MySQL)

Mr. DeRosa is the CEO of Syscall 7, LLC and the founder of ODA (onlinedisassembler.com), a collaborative reverse engineering platform in the cloud. He holds a Top Secret/SCI security clearance with a Full Scope Polygraph and has consulted for several 3-letter agencies within the US intelligence community over his 17 year career.

TECHNICAL SKILLS

- 17 years experience in embedded and system-level software development using C and assembly (x86, MIPS, PowerPC, ARM, NIOS II, and MicroBlaze)
- 17 years experience with software development environments (PyCharm, GDB, Eclipse, Visual Studio, American Arium, Lauterbach, Green Hills, Xilinx, and BDI)
- 17 years experience in device driver development (wired and wireless network interface controllers, compact flash cards, PCI, SPI, and I^2C)
- 17 years experience configuring and developing custom and commercial networking protocols, including the development of Wireshark dissectors in C
- 15 years experience in static and dynamic reverse engineering (IDA Pro, WinDbg, OllyDbg)
- 15 years experience in scripting languages (Python, Perl, Bash, Ruby)
- 10 years experience in higher level languages, including Python, C++, C#, and Java

CERTIFICATIONS

- Cisco Certified Network Associate (CCNA)
- GIAC Certified Penetration Tester (GPEN)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Firewall Analyst (GCFW)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Security Expert (GSE)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Security Essentials (GSEC)
- Certified Ethical Hacker (CEH)
- Certified Scrum Master (CSM)

EDUCATION

May 2009

M.S. IN ELECTRICAL AND COMPUTER ENGINEERING Baltimore, MD
The Johns Hopkins University GPA 4.0/4.0

B.S. IN COMPUTER ENGINEERING WITH C.S. DEPT. HONORS May 2003
Messiah College GPA 3.94/4.0 Grantham, PA

EMPLOYMENT

SYSCALL 7, LLC WOODBINE, MD
CEO and Principal Security Researcher JANUARY 2014 - PRESENT

- Founded Syscall 7 in 2014 and serves as Chief Executive Officer
- Established and manages all company operations, including hiring, human resources, technical management, and business development
- Grew the company to a strong team of 10 software developers and security researchers
- Led a security research team in performing security assessments on a range of embedded and mobile devices in the automotive, manufacturing, and medical industries
- Performed security research on Android-based mobile devices
- Developed the curriculum for a 3-day, hands-on course on reverse engineering and security analysis. Taught this public course to students coming from around the world for the past two years.
- Performed reverse engineering in support of technology-related litigation to identify the measures taken to protect trade secrets and intellectual property for embedded devices in the automotive, medical, and telecommunications industries
- Conducted vulnerability research and software security audits on optical and copper networking devices to identify security vulnerabilities in the firmware of the systems under investigation
- Developed fuzzers against networking platforms to identify potential security weaknesses in the protocol implementations on these devices
- Extracted firmware images from x86, PowerPC, and MIPS embedded devices using flash/EEPROM programmers such as DediProg and BP Microsystems in order to analyze the security of the system through a combination of static and dynamic reverse engineering
- Developed proof-of-concept manipulations to demonstrate the weaknesses uncovered on the devices under investigation
- Developed a custom SPI-based driver in C to enable port mirroring on an undocumented Broadcom chipset in order to enable further introspection of backplane traffic on an optical networking device under investigation
- Performed binary reverse engineering against custom computer systems running a variety of operating systems (Windows, Linux, VxWorks, and other proprietary systems) to identify vulnerabilities and security weaknesses
- Developed custom software tools in C, Python, and assembly to support CNE operations

- Conducted cybersecurity research and development to enable Computer Network Operations (CNO) and Computer Network Exploitation (CNE) for foreign intelligence collection
- Setup a lab environment in which to configure network infrastructure devices and simulate a variety of real-world networking scenarios. The devices in the lab included enterprise and ISP-grade network infrastructure devices such as firewalls, routers, and switches. The configuration scenarios included industry standard technologies like VPNs, VLANs, NAT, and PAT
- Implemented a custom communications protocol in Ruby as a plugin for an end-to-end communications framework built on Ruby-on-Rails
- Participated in the full lifecycle development of these tools from requirement analysis, design, and development to testing and maintenance support
- Used an Agile Scrum approach to software development with industry standard best practices of test-driven development, unit testing, continuous integration, and revision control (subversion and git)
- Created the Online Disassembler (ODA) website and lead a team of developers to develop the Django-based backend framework of the website. Wrote the backend Python wrapper to access the native BFD shared library, which provides the disassembly engine. Integrated a prototype for dynamic runtime analysis of packed binaries into ODA by customizing and patching the open source Cuckoo virtual sandboxing platform. Assisted in website UI design and contributed new features on both the client-side and server-side code base.

INTELESYS CORPORATION	ELKRIDGE, MD
Senior Firmware Engineer	JUNE 2010 – March 2015

- Conducted software security audits of electrical power critical infrastructure (SCADA) systems
- Developed proof-of-concept manipulations against these systems to demonstrate the severity of the weaknesses uncovered
- Provided guidance on security critical infrastructure systems to defend against the weaknesses identified and mitigate their risks
- Reverse engineered proprietary network protocols and developed Wireshark dissectors to parse them. Identified security weaknesses of these protocols and wrote proof-of-concept manipulations against them.
- Performed software security audits of networking devices to identify weaknesses in their booting mechanisms and runtime operations
- Designed and developed MIPS and x86 firmware for custom, embedded devices.
- Developed a Linux-based IP tunneling solution using the TUN/TAP virtual network kernel devices.
- Developed distributed processing frameworks based on RPC technologies.
- Wrote a Python utility to extract over 300 features from Windows PE executables, which were then processed by an automated malware analysis platform

EVI TECHNOLOGY / EDO CORP. / ITT CORP. COLUMBIA, MD
Senior Firmware Engineer APRIL 2005 – JUNE 2010

- Analyzed software on Windows and a variety of embedded platforms with IDA Pro
- Designed and developed a portable architecture for an embedded, non-multitasking kernel comprising a device driver framework, network stack, and filesystem ported to a variety of embedded networking platforms.
- Developed device drivers for UARTs, compact flash devices, and network interface controllers (both wired and wireless).
- Developed system-level code for exception handling and virtual memory management.
- Developed the VHDL firmware for a CPLD used to bootstrap a Xilinx FPGA. Developed bootloaders for a variety of platforms.
- Developed Wireshark/Ethereal dissectors for custom network protocols.
- Developed and maintained the SCons (Python-based) build system used for building our cross-platform code.
- Served as team technical lead and supervisor of a small team of engineers.

U.S. DEPARTMENT OF NAVY (NAWCAD/NAVAIR) PATUXENT RIVER, MD
Computer Engineer JUNE 2003 – APRIL 2005

- Developed a variety of Windows and VMS-based applications in various programming languages (C, C++, C#, Visual Basic) to support the infrastructure of a flight simulation laboratory.
- Wrote a 1553 bus controller in C to simulate an aircraft mission computer.
- Integrated RADAR and FLIR image generators with aircraft avionics.
- Implemented a C#- based multi-platform simulation executive.
- Designed and developed a Windows DLL to transmit real-time simulation data as a PCM data stream over fiber to a telemetry processing facility.

PUBLICATIONS

- https://medium.com/hackernoon/finally-a-use-for-my-crypto-wallet-66250af48728
- https://syscall7.com/android-device-hardening
- https://syscall7.com/machine-emulation-with-ghidra
- https://syscall7.com/securing-your-product